



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/757,963	01/10/2001	John S. Flowers	HVWD-01008US0 MEM/SBS	9385
758	7590	05/25/2004	EXAMINER	
FENWICK & WEST LLP SILICON VALLEY CENTER 801 CALIFORNIA STREET MOUNTAIN VIEW, CA 94041			MOORTHY, ARAVIND K	
			ART UNIT	PAPER NUMBER
			2131	21

DATE MAILED: 05/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/757,963

Applicant(s)

FLOWERS ET AL.

Examiner

Aravind K Moorthy

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 April 2004.
2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 5-13, 15-25, 27-37, 39 and 40 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 5-13, 15-25, 27-37, 39 and 40 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on 10 January 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 18.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 5-13, 15-25, 27-37, 39 and 40 are pending in the application.
2. Claims 5-13, 15-25, 27-37, 39 and 40 have been rejected.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/30/04 has been entered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Art Unit: 2131

4. Claims 5, 8, 12, 13, 15-17, 20, 24, 25, 27-29, 32, 36, 37, 39 and 40 are rejected under 35 U.S.C. 102(e) as being anticipated by Teal U.S. Patent No. 6,477,651 B1.

As to claims 5, 17 and 29 Teal discloses a vulnerability detection system (VDS) (i.e. data collector) for gathering information about the network to determine vulnerabilities of a plurality of hosts on the network. Teal discloses an intrusion detection system (IDS), cooperative with the VDS, for examining network traffic responsive to the vulnerabilities of a host from the plurality of hosts as determined by the VDS to detect traffic indicative of malicious activity [column 4, lines 28-58].

As to claims 8, 20 and 32, Teal discloses a vulnerabilities rules database, in communication with the VDS, for storing rules describing vulnerabilities of the plurality of hosts. Teal discloses that the VDS is adapted to analyze the gathered information with the rules to determine the vulnerabilities of the plurality of hosts [column 4, lines 48-58].

As to claims 12, 24 and 36, Teal discloses an intrusion rules database in communication with the IDS, for storing rules describing malicious activity. Teal discloses that the IDS is adapted to analyze the network traffic with the rules to detect network traffic indicative of exploitations of the determined vulnerabilities [column 4, lines 28-47].

As to claims 13, 25 and 37, Teal discloses that the IDS is adapted to detect traffic indicative of exploitations of only the determined vulnerabilities [column 4 line 59 to column 5 line 8].

As to claims 15, 16, 27, 28, 39 and 40, Teal discloses that the VDS is adapted to update the determined vulnerabilities and that the IDS is adapted to detect traffic indicative of malicious

Art Unit: 2131

activity in response to the update. Teal discloses that the VDS is adapted to update the determined vulnerabilities in response to a change in the network [column 5, lines 9-35].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 6, 7, 18, 19, 30 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teal U.S. Patent No. 6,477,651 B1 as applied to claims 5, 17 and 29 above, and further in view of Shostack et al U.S. Patent No. 6,298,445 B1.

As to claims 6, 7, 18, 19, 30 and 31, Teal does not teach that the VDS is adapted to gather information about the network by sending data to the plurality of hosts and receiving responsive data from the plurality of hosts. Teal does not teach that the VDS is adapted to gather information automatically provided by the plurality of hosts.

Shostack et al teaches a VDS that is adapted to gather information about the network by sending data to the plurality of hosts and receiving responsive data (i.e. pinging) from the plurality of hosts [column 7, lines 11-19]. Shostack et al teaches that the VDS is adapted to gather information automatically provided by the plurality of hosts [column 7, lines 31-35].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Teal so the VDS would have adapted to gather information about the network by sending data to the plurality of hosts and receiving responsive data (i.e. pinging) from the plurality of hosts.

Art Unit: 2131

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Teal by the teaching of Shostack et al because it automatically provides, in real-time, software enhancements with updated information regarding security vulnerabilities. It enables a system administrator to implement prevention techniques before a security breach occurs [column 2, lines 31-47].

6. Claims 9-11, 21-23 and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teal U.S. Patent No. 6,477,651 B1 as applied to claims 5, 17 and 29 above, and further in view of Gleichauf et al U.S. Patent No. 6,415,321 B1.

As to claims 9-11, 21-23 and 33-35, Teal does not teach that the VDS is adapted to analyze the gathered information with the rules to identify operating systems on the plurality of hosts and determine the vulnerabilities responsive to the respective operating systems. Teal does not teach that the VDS is adapted to analyze the gathered information with the rules to identify open ports on the plurality of hosts and determine the vulnerabilities based on the open ports. Teal does not teach that the VDS is adapted to analyze the gathered information with the rules to identify applications executing on the plurality of hosts and determine the vulnerabilities based on the applications.

Gleichauf et al teaches that the VDS is adapted to analyze the gathered information with the rules to identify operating systems on the plurality of hosts and determine the vulnerabilities responsive to the respective operating systems [column 5, lines 15-31]. Gleichauf et al teaches that the VDS is adapted to analyze the gathered information with the rules to identify open ports on the plurality of hosts and determine the vulnerabilities based on the open ports [column 5, lines 15-31]. Gleichauf teaches that the VDS is adapted to analyze the gathered information with

Art Unit: 2131

the rules to identify applications executing on the plurality of hosts and determine the vulnerabilities based on the applications [column 6, lines 48-65].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Teal so the VDS would have been able to analyze the gathered information to identify operating systems, open ports, and applications on the plurality of hosts to determine the vulnerabilities based on the operating systems, open ports, and applications.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Teal by the teaching of Gleichauf et al because the examiner asserts that certain operating systems and applications running on a computer are more open to attacks. The examiner asserts that open ports make a computer more vulnerable to attacks.


Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
May 20, 2004


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100